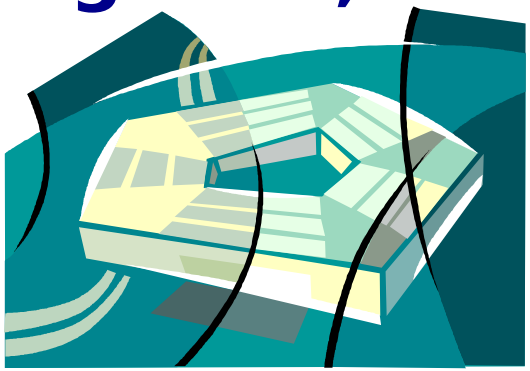
GAO
Accountability * Integrity * Reliability

Gauging an IT Organization's Maturity: Overview of GAO's Approach

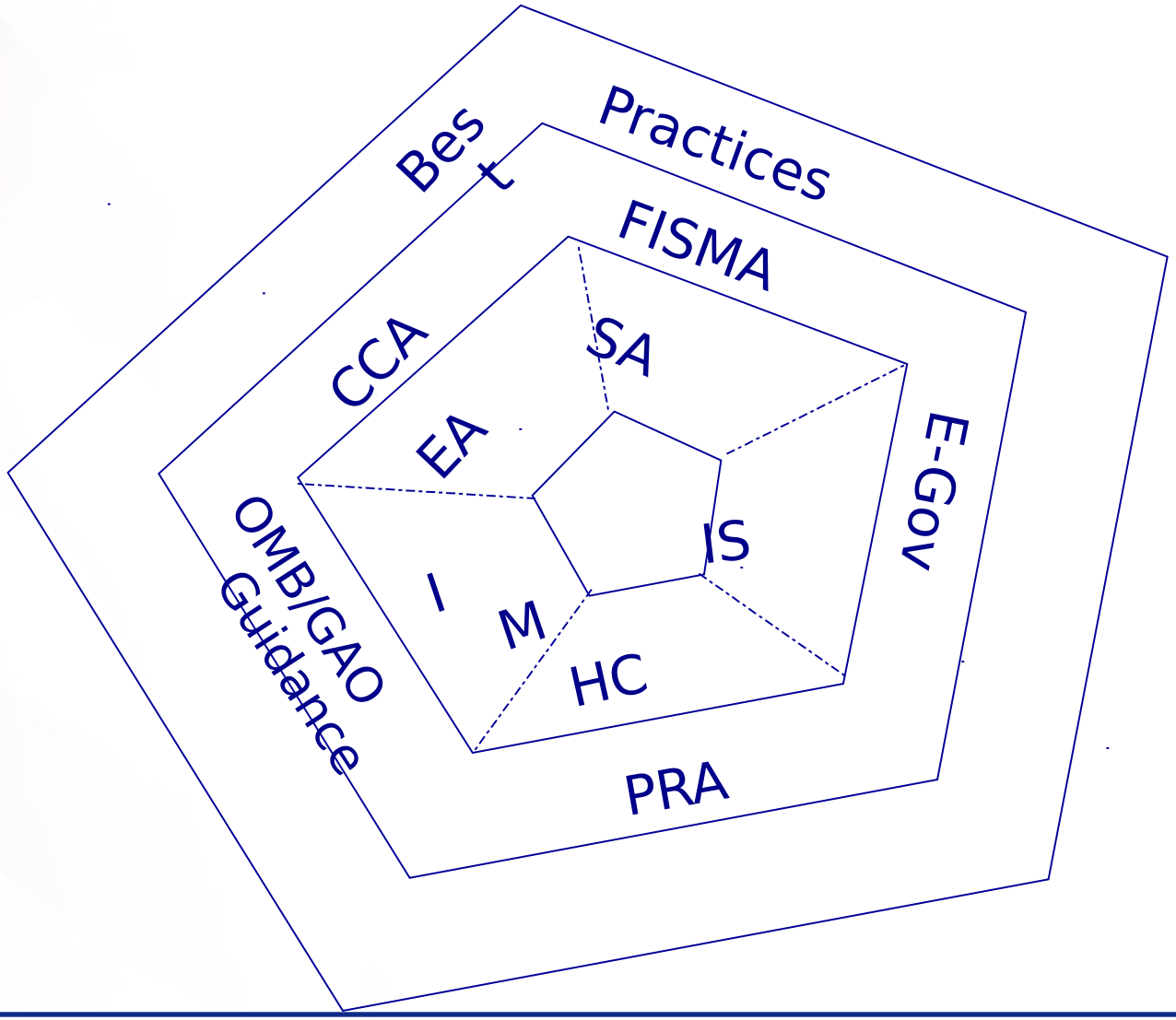
Briefing to ASD/NII Staff
August 2, 2007



Agenda

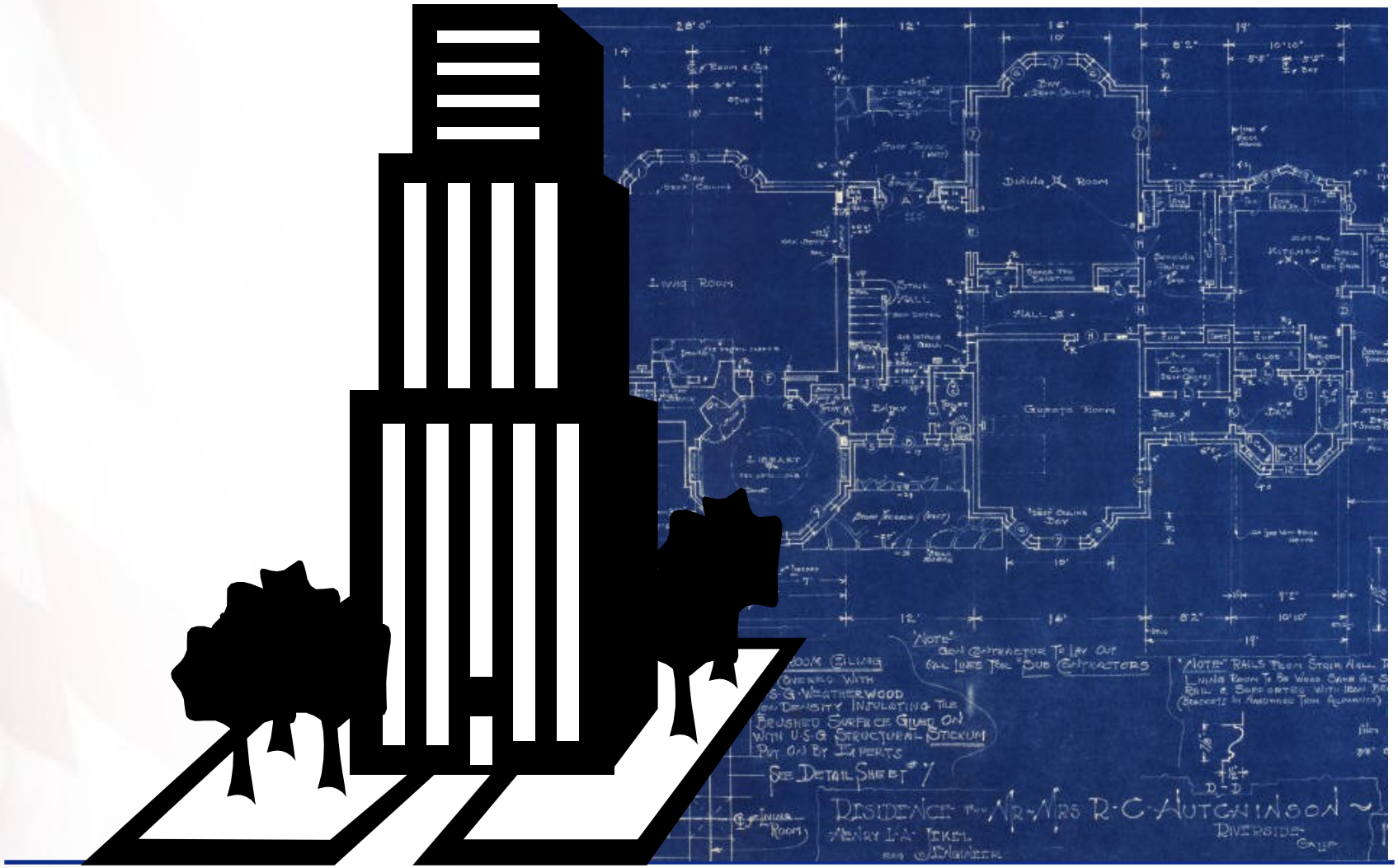
- Introduction
- Enterprise Architecture
- Investment Management
- Systems Acquisition/Development
- IT Human Capital Management
- Information Security
- Questions

Introduction



Enterprise Architecture

GAO
Accountability * Integrity * Reliability



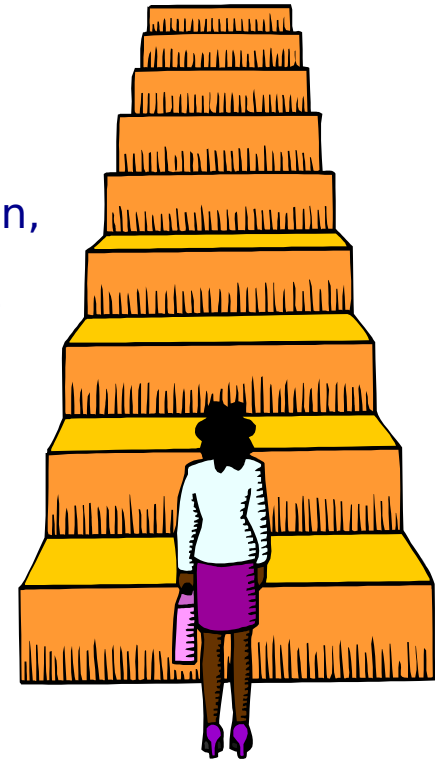
General Approach

An EA audit generally includes:

1. Application of the **EAMMF framework** to:
   - Determine the extent to which an organization has adopted key elements of architecture management best practices by comparing program documentation, such as program policies and procedures, steering and executive committee charters, and architecture products, to elements in the framework.

2. Analysis of the **"content"** of agency documents to:
   - Determine the level of compliance with all federal accounting, financial management, and reporting requirements.
   - Examine the content of the "As Is" and "To Be" environments.
   - Assess the content of the transition plan to include time-

     phased milestones for phasing out existing systems, resource needs for implementing the "To Be" environment, and information on the systems inventory.



See GAO-03-584G

EA Management Maturity Framework

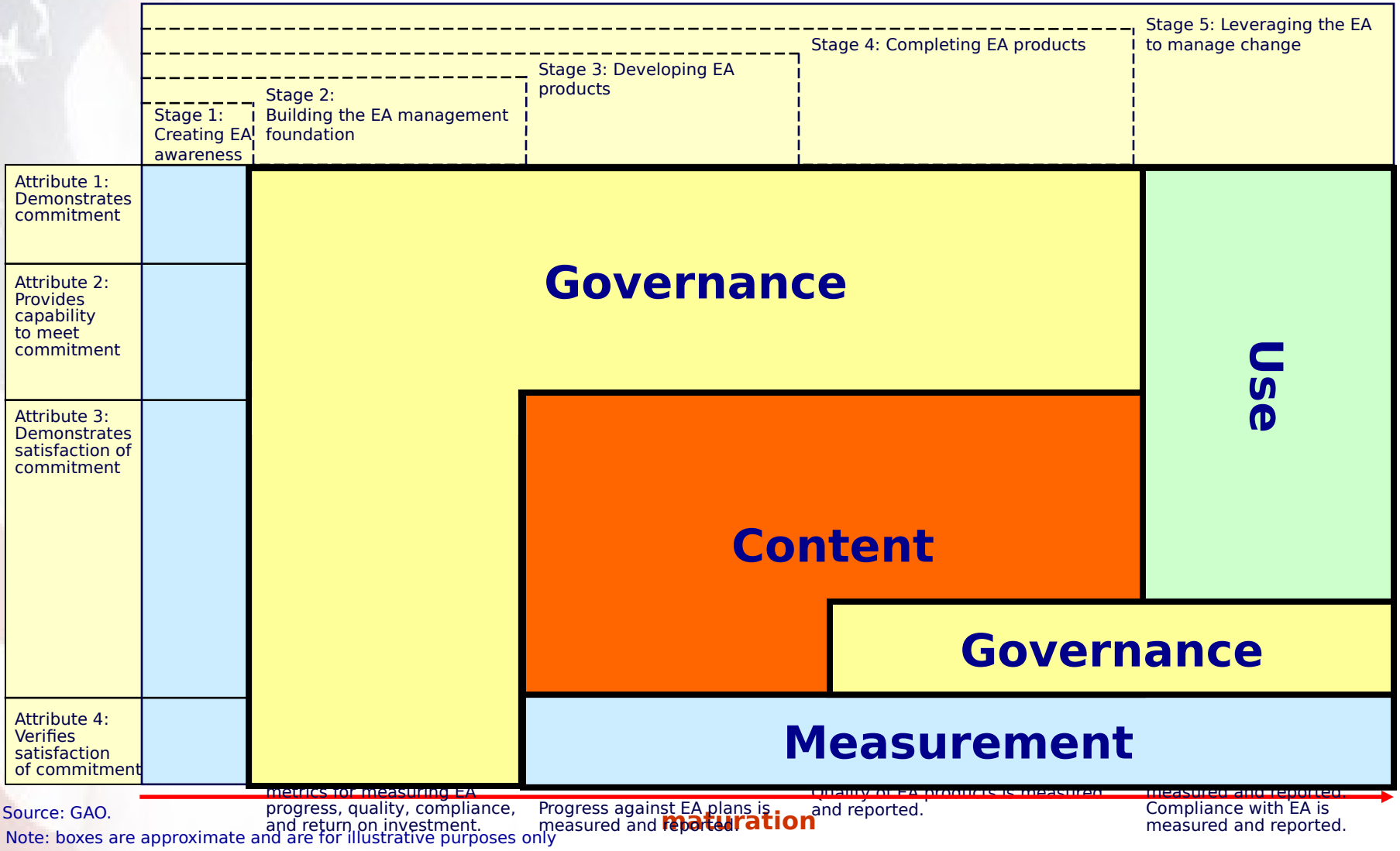
	Stage 1: Creating EA awareness	Stage 2: Building the EA management foundation	Stage 3: Developing EA products	Stage 4: Completing EA products	Stage 5: Leveraging the EA to manage change
Attribute 1: Demonstrates commitment		Adequate resources exist. Committee or group representing the enterprise is responsible for directing, overseeing, and approving EA.	Written and approved organization policy exists for EA development.	Written and approved organization policy exists for EA maintenance.	Written and approved organization policy exists for IT investment compliance with EA.
Attribute 2: Provides capability to meet commitment		Program office responsible for EA development and maintenance exists. Chief architect exists. EA being developed using a framework, methodology, and automated tool.	EA products are under configuration management.	EA products and management processes undergo independent verification and validation.	Process exists to formally manage EA change. EA is integral component of IT investment management process.
Attribute 3: Demonstrates satisfaction of commitment		EA plans call for describing both the "as-is" and the "to-be" environments of the enterprise, as well as a sequencing plan for transitioning from the "as-is" to the "to-be." EA plans call for describing both the "as-is" and the "to-be" environments in terms of business, performance, information/data, application/service, and technology. EA plans call for business, performance, information/data, service, and technology descriptions to address security.	EA products describe or will describe both the "as-is" and the "to-be" environments of the enterprise, as well as a sequencing plan for transitioning from the "as-is" to the "to-be." Both the "as-is" and the "to-be" environments are described or will be described in terms of business, performance, information/data, application/service, and technology. Business, performance, information/data, application/service, and technology descriptions address or will address security.	EA products describe both the "as-is" and the "to-be" environments of the enterprise, as well as a sequencing plan for transitioning from the "as-is" to the "to-be." Both the "as-is" and the "to-be" environments are described in terms of business, performance, information/data, application/service, and technology. Business, performance, information/data, application/service, and technology descriptions address security. Organization CIO has approved current version of EA. Committee or group representing the enterprise or the investment review board has approved current version of EA.	EA products are periodically updated. IT investments comply with EA. Organization head has approved current version of EA.
Attribute 4: Verifies satisfaction of commitment		EA plans call for developing metrics for measuring EA progress, quality, compliance, and return on investment.	Progress against EA plans is measured and reported.	Quality of EA products is measured and reported.	Return on EA investment is measured and reported. Compliance with EA is measured and reported.

maturation

Source: GAO.

Note: each stage includes all elements of previous stages.

EAMMF Groups

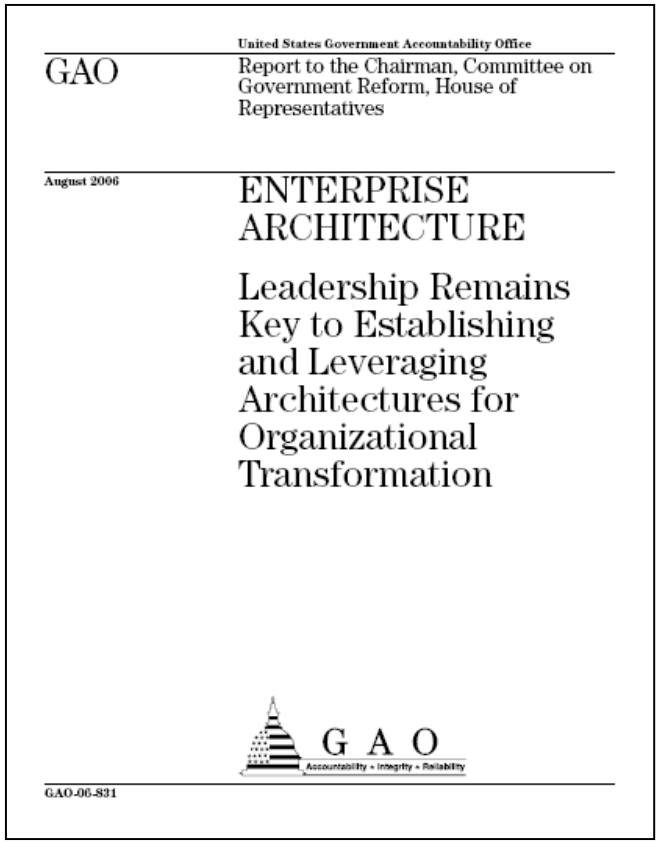

Stage 1: Creating EA awareness
Stage 2: Building the EA management foundation
Stage 3: Developing EA products
Stage 4: Completing EA products
Stage 5: Leveraging the EA to manage change
Attribute 1: Demonstrates commitment
Attribute 2: Provides capability to meet commitment
Attribute 3: Demonstrates satisfaction of commitment
Attribute 4: Verifies satisfaction of commitment
Governance
Use
Content
Governance
Measurement
metrics for measuring EA progress, quality, compliance, and return on investment.
Progress against EA plans is measured and reported.
Quality of EA products is measured and reported.
measured and reported.
Compliance with EA is measured and reported.
maturation

Source: GAO.

Note: boxes are approximate and are for illustrative purposes only

Application of the EAMMF Framework

- In 2006, we surveyed 28 EA programs at 27 major federal departments and agencies using a questionnaire based on our EAMMF. We then reviewed the survey responses and supporting documentation to verify each agency's satisfaction of the 31 EAMMF elements.



United States Government Accountability Office

GAO

Report to the Chairman, Committee on Government Reform, House of Representatives

August 2006

ENTERPRISE ARCHITECTURE

Leadership Remains Key to Establishing and Leveraging Architectures for Organizational Transformation

GAO

Accountability * Integrity * Reliability

GAO-06-831

See GAO-06-831

Application of the EAMMF Framework

Sample Evaluation Criteria

Committee or group representing the enterprise is responsible for directing, overseeing, and approving EA. (Stage 2)

- Does the agency have a chartered committee or group composed of representatives from across the enterprise, that is responsible for directing, overseeing, and approving the EA? Do meeting minutes exist that verify that the committee is meeting periodically and executing its designated responsibilities?

EA being developed using a framework, methodology, and automated tool. (Stage 2)

- Does an enterprise architecture methodology exist that defines how the enterprise is to develop, maintain, and validate enterprise architecture products? Does the methodology prescribe the standards, steps, tools, techniques, and measures to be used to provide reasonable assurance that expected product quality it attained?

Application of the EAMMF Framework

Sample Evaluation Criteria

EA products are under configuration management (Stage 3)

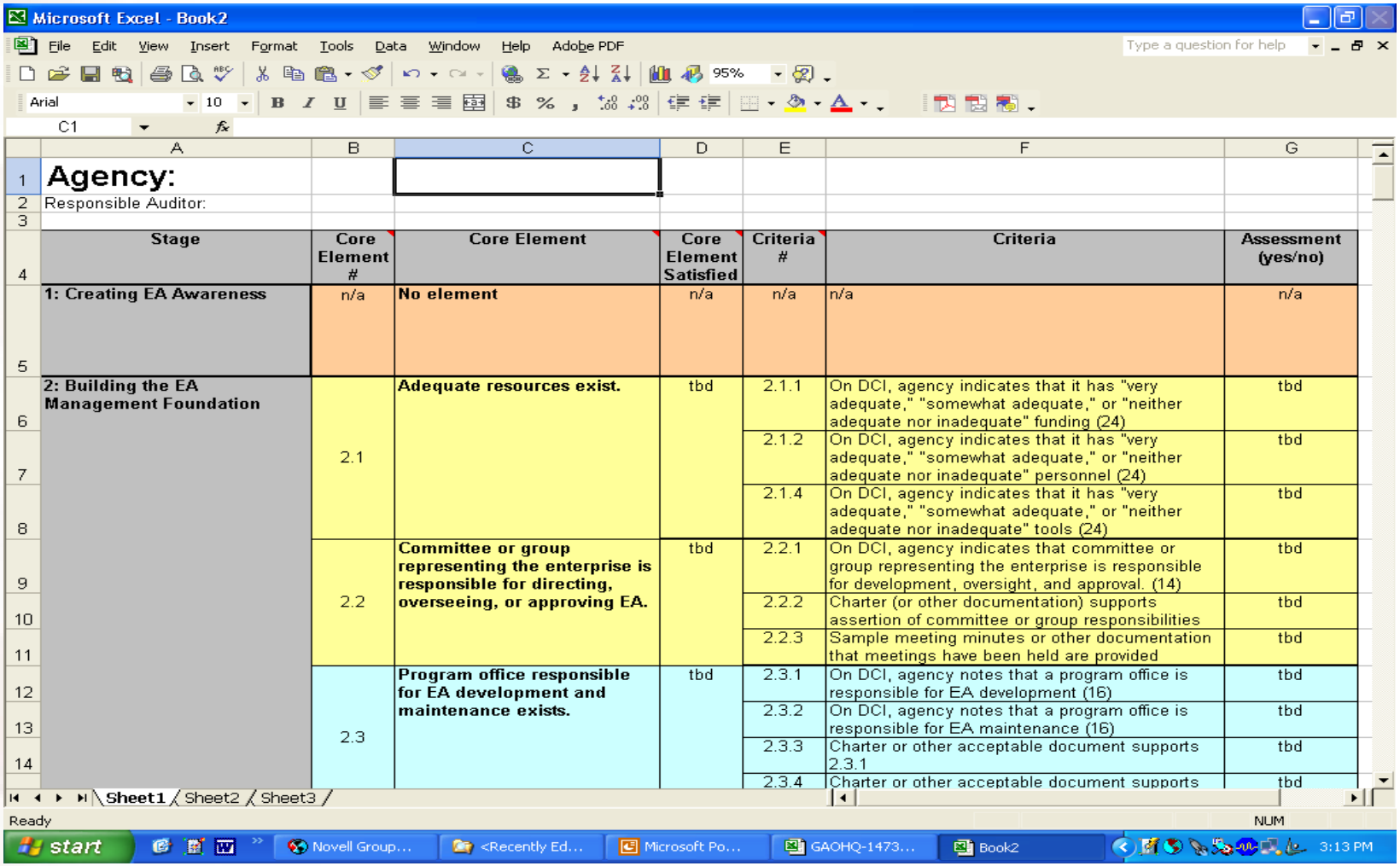
- Does a configuration management plan exist that describes how EA configuration items are identified, controlled, and audited? Do documents exist that verify that the configuration management process is being executed according to plan?

Progress against EA plans is measured and reported (Stage 3)

- Does an EA program plan against which progress can be measured? Is progress against this plan measured and reported? Does the agency take action to address deviations from the plan?

Application of the EAMMF Framework

GAO
Accountability * Integrity * Reliability



Microsoft Excel - Book2

File Edit View Insert Format Tools Data Window Help Adobe PDF

Type a question for help

Arial 10 B I U

C1

	A	B	C	D	E	F	G
1	**Agency:**						
2	Responsible Auditor:						
3							
4	**Stage**	**Core Element #**	**Core Element**	**Core Element Satisfied**	**Criteria #**	**Criteria**	**Assessment (yes/no)**
5	**1: Creating EA Awareness**	n/a	**No element**	n/a	n/a	n/a	n/a
6	**2: Building the EA Management Foundation**	2.1	**Adequate resources exist.**	tbd	2.1.1	On DCI, agency indicates that it has "very adequate," "somewhat adequate," or "neither adequate nor inadequate" funding (24)	tbd
7					2.1.2	On DCI, agency indicates that it has "very adequate," "somewhat adequate," or "neither adequate nor inadequate" personnel (24)	tbd
8					2.1.4	On DCI, agency indicates that it has "very adequate," "somewhat adequate," or "neither adequate nor inadequate" tools (24)	tbd
9		2.2	**Committee or group representing the enterprise is responsible for directing, overseeing, or approving EA.**	tbd	2.2.1	On DCI, agency indicates that committee or group representing the enterprise is responsible for development, oversight, and approval. (14)	tbd
10					2.2.2	Charter (or other documentation) supports assertion of committee or group responsibilities	tbd
11					2.2.3	Sample meeting minutes or other documentation that meetings have been held are provided	tbd
12		2.3	**Program office responsible for EA development and maintenance exists.**	tbd	2.3.1	On DCI, agency notes that a program office is responsible for EA development (16)	tbd
13					2.3.2	On DCI, agency notes that a program office is responsible for EA maintenance (16)	tbd
14					2.3.3	Charter or other acceptable document supports 2.3.1	tbd
					2.3.4	Charter or other acceptable document supports	tbd

Sheet1 Sheet2 Sheet3

Ready NUM

start Novell Group... <Recently Ed... Microsoft Po... GAOHQ-1473... Book2 3:13 PM

Application of the EAMMF Framework

- Agencies are automatically placed in stage 1.
- Agencies must satisfy all aspects of an element to fully satisfy the element. If an agency satisfies none of these requirements, the element is “not satisfied.” If an agency satisfies at least some of the requirements, the element is “partially satisfied.”
- Agencies must satisfy all elements of one stage to advance to the next maturity stage.
  - For example, if an agency satisfies all elements in stages 3-5, but has not used an enterprise architecture methodology to develop their architecture, they are still in stage 1. This ensures that a strong EA foundation is laid at every maturity level.
- Different views of agency maturity include:
  - overall satisfaction of framework elements;
  - satisfaction of framework elements within individual stages or groups; and
  - Agency maturity stage, when agencies allowed to advance to the next stage by only partially satisfying a framework element.

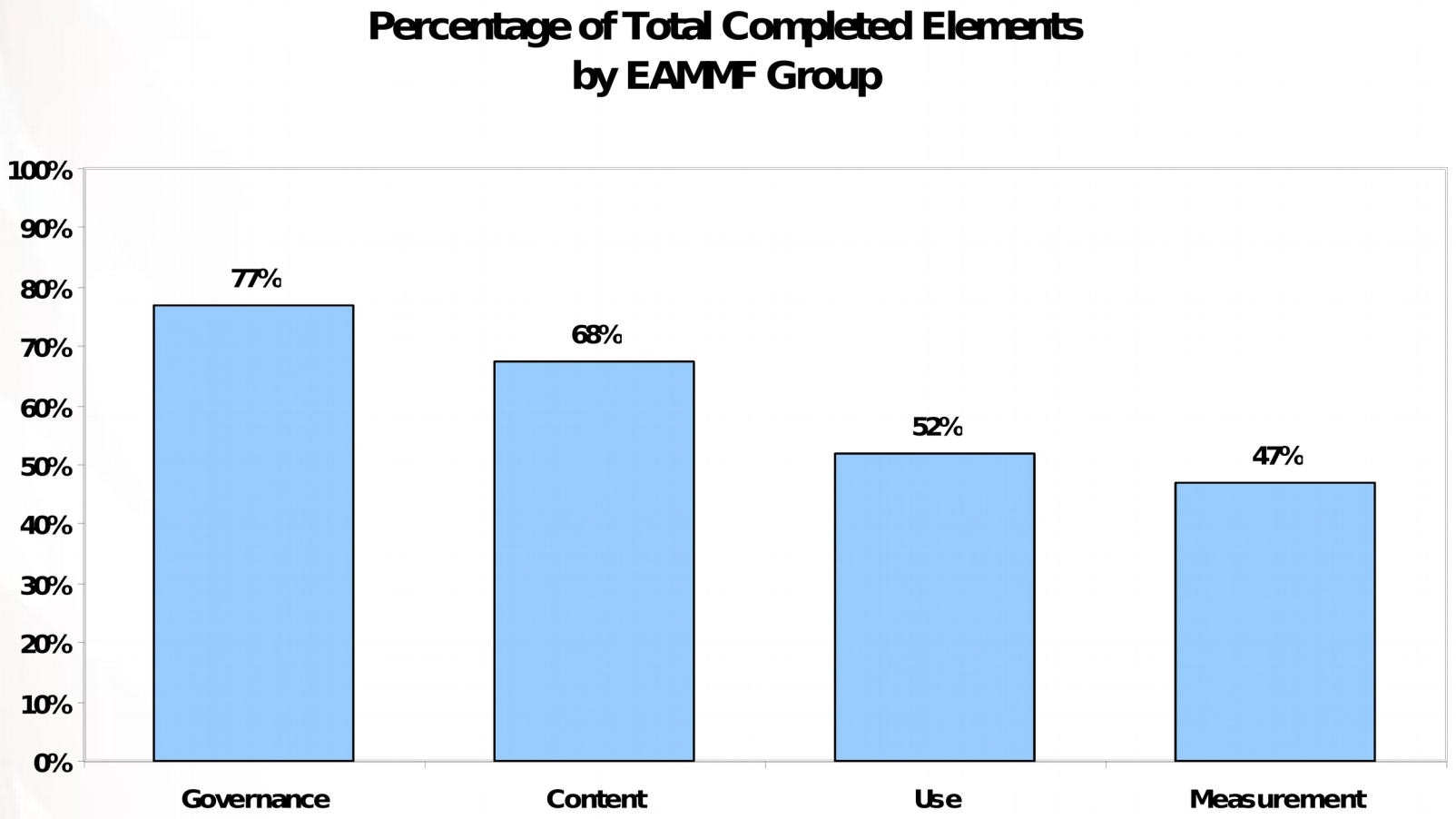
State of Federal Agencies

	Stage 1	Stage 2: Building the EA management foundation	Percent Satisfying Element
Attribute 1: Demonstrates commitment		**Adequate resources exist.** **Committee or group representing the enterprise is responsible for directing, overseeing, and approving EA.**	**86** **57**
Attribute 2: Provides capability to meet commitment		**Program office responsible for EA development and maintenance exists.** **Chief architect exists.** **EA being developed using a framework, methodology, and automated tool.**	**93** **96** **61**
Attribute 3: Demonstrates satisfaction of commitment		**EA plans call for describing both the "as-is" and the "to-be" environments of the enterprise, as well as a sequencing plan for transitioning from the "as-is" to the "to-be."** **EA plans call for describing both the "as-is" and the "to-be" environments in terms of business, performance, information/data, application/service, and technology.** **EA plans call for business, performance, information/data, service, and technology descriptions to address security.**	**93** **93** **89**
Attribute 4: Verifies satisfaction of commitment		**EA plans call for developing metrics for measuring EA progress, quality, compliance, and return on investment.**	**50**

maturation

Source: GAO.

State of Federal Agencies



Source: GAO-06-831

EA Content Analysis

- **Key architecture products**
  - "As-Is" EA products describe the current environment
  - "To-Be" EA products describe the target environment
  - Transition plan

EA Content Analysis

- **General analysis covers:**
  - Completeness
  - Integration
  - Consistency
  - Utility

- **Specific analysis e.g.,**
  - Assess the extent to which EA addresses the requirements in public law
  - Assess whether or not EA can be used to guide IT investment management
  - Assess whether or not EA can be used to address information sharing issues
  - Assess whether or not EA can be used to guide application development and system integration

Department of Homeland Security: Enterprise Architecture Content

- In 2004, we reported on the completeness and usability of the initial version of Department of Homeland Security's (DHS) EA.
- In summary, we found that while the initial version provided a foundation on which to build, it was missing important content (i.e., was not sufficiently complete), which limited its usability.
- Moreover, we found that this version was not systematically derived from a DHS or national homeland security business strategy, but rather was an amalgamation of the existing architectures that several of DHS's predecessor agencies already had, along with their respective portfolios of system investments.
- Accordingly, we made 41 recommendations.

See GAO-04-777

Department of Homeland Security: Enterprise Architecture Content

- In May 2007, we reported that the third version of the DHS EA had evolved beyond prior versions, but missing architecture content constrained its usability.

- The full depth and breadth of EA content that our recommendations provided for was still missing. For example,
  - the DHS EA 2006 does not describe data management processes and procedures, such as ones for identifying and standardizing core data elements to be used across DHS and with external stakeholders,
  - while the EA provides a data dictionary, it does not include definitions of all key terms (e.g., first responder),
  - the EA does not describe the interfaces between enterprise applications and application components. For example, it does not depict the interconnection involved between the “Communicate Risks” and “Threats to the Public” business functions, and
  - the DHS EA did not include a transition plan, and it did not include any evidence of a gap analysis—a comparison of the “as-is” and “to-be” architectures to identify capability differences.

- We made recommendations to ensure that DHS fully implements our prior EA recommendations and effectively solicits stakeholder comments on future versions of its EA.

- DHS has since issued a new version of its EA.

See GAO-07-564

Investment Management

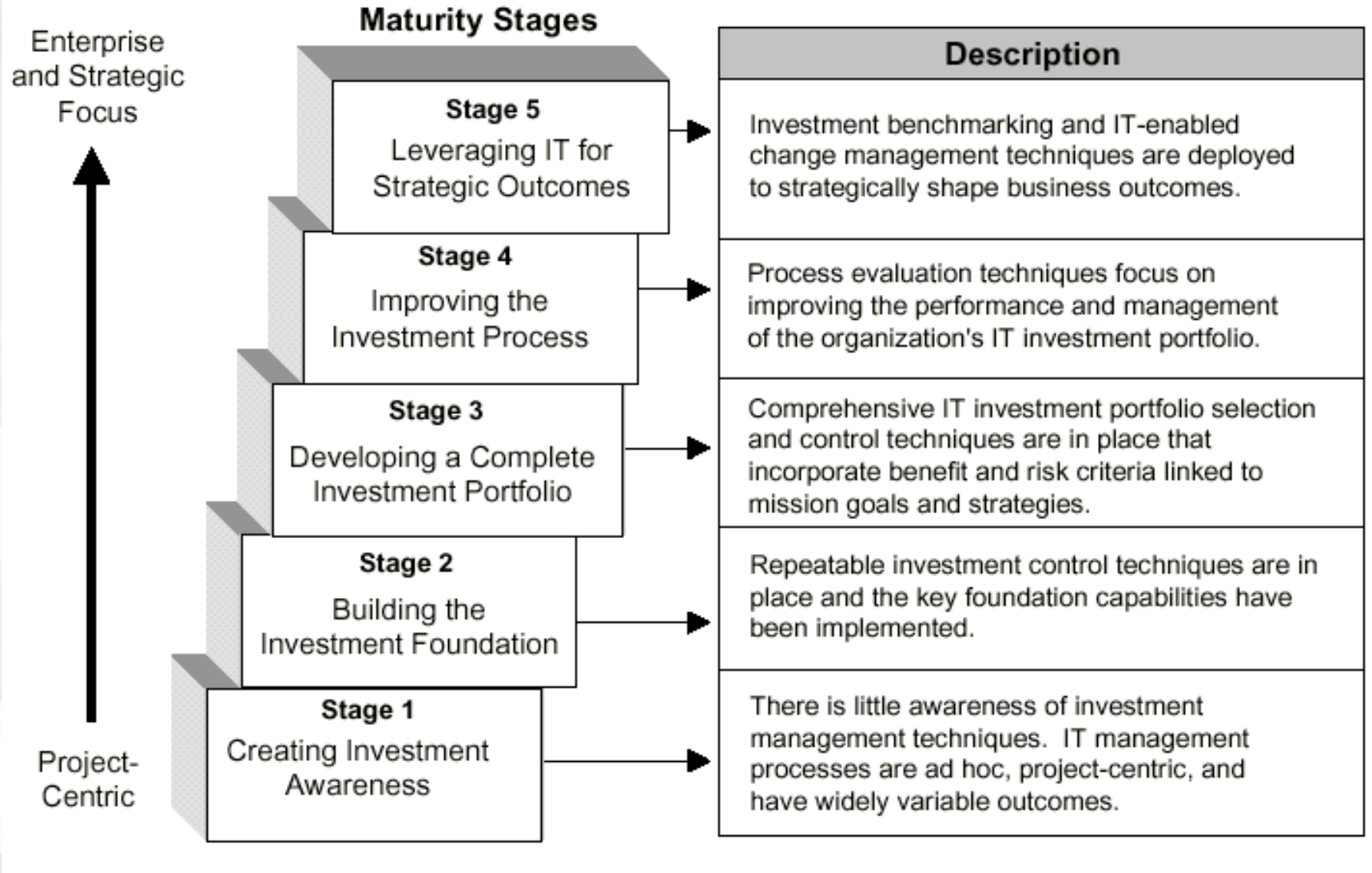
What is the ITIM?

- Information Technology Investment Management (**ITIM**) Framework
- Five stage maturity model
- Written for use in all agencies with appropriate interpretation
- Addresses process maturity for IT investment management
  - Broadly generalizes investment decision making
- Technology/implementation neutral
  - Choose your own implementation strategy

How is it used?

- GAO guidance for conducting assessments
- Agency use for conducting self-assessments
  - Static assessment of maturity
  - Measure progress over time
- Provide framework for understanding relationship among processes
  - Implement using techniques that work for specific agency
    - Being used by several agencies

IT Investment Management Framework


Maturity Stages
Enterprise and Strategic Focus
Project-Centric
Stage 5
Leveraging IT for Strategic Outcomes
Stage 4
Improving the Investment Process
Stage 3
Developing a Complete Investment Portfolio
Stage 2
Building the Investment Foundation
Stage 1
Creating Investment Awareness
Description
Investment benchmarking and IT-enabled change management techniques are deployed to strategically shape business outcomes.
Process evaluation techniques focus on improving the performance and management of the organization's IT investment portfolio.
Comprehensive IT investment portfolio selection and control techniques are in place that incorporate benefit and risk criteria linked to mission goals and strategies.
Repeatable investment control techniques are in place and the key foundation capabilities have been implemented.
There is little awareness of investment management techniques. IT management processes are ad hoc, project-centric, and have widely variable outcomes.

ITIM's Structure

- **Maturity Stage**
  Ex. Stage 2: Building the Investment Foundation
- **Critical Process**
  Ex. Selecting an Investment
- **Key Practices**
  - *Organizational Commitments (e.g.* senior management sponsorship and policies and procedures)
  - *Prerequisites* (e.g. resources, structures and training)
  - *Activities* (e.g. performing and tracking the work and taking corrective actions)

IT Investment Management Reviews

DHS: Findings, Recommendations, and Results

- In 2007, evaluated the investment management capabilities of DHS, the third highest IT spender in the federal government.
- **Findings**: DHS has the management structures needed to manage its business systems investment. It has an executive investment review board, and several project- level policies and procedures in place. However, the department lacks policies and procedures for developing criteria for selecting and reselecting investments and managing the oversight of IT projects. It also does not have a mature process for managing its IT investments as a portfolio.
- **Recommendations**: We recommended that the department fully define the policies and procedures associated with project-level and portfolio-level investment management as discussed in our report.
- **Results**: Since the report was recently issued, the recommendations remain open.

Information Technology: DHS Needs to Fully Define and Implement Policies and Procedures for Effectively Managing Investments, GAO-07-424 (Apr. 14, 2007)

IT Investment Management Reviews

Governmentwide: Findings, Recommendations, and Results

- In January 2004, we reported on mixed results of federal agencies' use of IT investment management practices.
- **Findings**: Although most of the agencies had IT investment boards responsible for defining and implementing the agencies' IT investment processes, none had fully implemented practices for monitoring the progress of its investments.
- **Recommendations**: GAO made over 200 recommendations to the 26 agencies. These recommendations addressed issues such as developing policies and procedures, improving processes for effective oversight, and requiring post-implementation reviews to be completed.
- **Results**: Over one-third of these recommendations have been fully addressed and others are being actively addressed.

Information Technology Management: Governmentwide Strategic Planning, Performance Measurement, and Investment Management Can Be Further Improved, GAO-04-49 (Jan. 12, 2004)

Systems & Services Acquisition/Development

Systems & Services Acquisition/Development

- Establishing standard institutional definitions around acquisition/ development processes and practices (e.g., risk management, performance management).

- Achieving better project cost and schedule performance and developing higher quality products.

- Execution of these processes and practices (e.g., requirements development, quality assurance).

We and others, such as Carnegie Mellon University's Software Engineering Institute (SEI), have identified and promoted the use of a number of best practices associated with acquiring IT systems and services.

Systems Acquisition/Development

Among the best practices we use to examine system acquisitions are:

- Acquisition planning—plans are prepared during planning phase and maintained throughout acquisition. These plans address the entire acquisition process as well as life cycle support and responsibility for planning activities is designated.
- Architectural alignment—ensure that the acquisition is consistent with the organization's enterprise architecture.
- Contract tracking and oversight—activities are planned for and conducted to ensure that the acquiring organization has sufficient insight into the contractor's activities to manage and control the contractor and to ensure contract requirements are met.
- Economic Justification—ensure that the acquisition has an adequate examination of cost, expected benefits, and anticipated risks.
- Evaluation—activities are planned for and conducted to ensure that evidence that contract products satisfy defined requirements is provided prior to acceptance of contractor products.

Systems Acquisition/Development

- Project management—activities are planned for and conducted to ensure that the project office manages and controls project cost and schedule and addresses any problems that occur.
- Requirements development and management—contractual requirements are developed, managed, and maintained; also that stakeholders understand these requirements.
- Risk management—process that provides for the identification, analysis, and mitigation of risks and that projectwide identification and mitigation of risks is encouraged.
- Solicitation—process by which contractual requirements and other evaluation criteria are used to judge which contractor and/or product will best meet the users' needs.
- Transition to support—process to plan for the movement of a finished acquisition product from the acquiring organization to a support organization.

Systems Acquisition/Development

In addition, we have several best practices specifically related to commercial component-based business system acquisitions:

- Component modification—ensure that modification of commercial components is allowed only based on a thorough analysis of life-cycle costs and benefits.
- Dependency analysis—ensures that acquisition decisions are based on deliberate and thorough research, analysis, and evaluation of component's interdependencies.
- Legacy system integration planning—explicit provision of time and resources for integrating new components and legacy systems.
- Organization change management—explicit provision for preparing users for the impact of new components/systems on the embedded business processes and user roles and responsibilities.

Systems Acquisition/Development

- Tradeoff analysis—examines the tradeoffs among the availability of commercial products (current and future), the architectural environment in which the system is to operate (current and future), system requirements, and cost and schedule constraints.
- Vendor/product research and evaluation—examines and tests component and vendor options both early (prior to acquisition) and continuously, based on defined system requirements and vendor/commercial product characteristics.

Services Acquisition

Finally, we have several best practices specifically related to acquisition of information technology services:

- Determine sourcing strategy—determine whether internal or external expertise can best meet IT needs
- Define operational model—formalize executive leadership, team composition, client responsibilities, and operating relationships between client and provider organizations
- Develop contract—establish the legal terms for the outsourcing relationship

Services Acquisition

- Select provider—find one or more providers who can help them reach their IT outsourcing goals
- Transition to provider—transfer responsibility for IT function(s) to one or more providers
- Manage provider performance—ensure provider is meeting performance requirements
- Ensure services are provided—make sure that end user needs are met and services provided.

Internal Revenue Service: System Acquisition/Development

Determine whether IRS had

(1) established adequate requirements development and management policies and procedures and

(2) whether IRS has used effective requirements development and management practices on its system development efforts.

- Reviewed BSM requirements development and management policies, procedures, guidance, and tools.
- Analyzed requirements-related documentation from the following BSM projects:
  - Customer Account Data Engine (CADE) release 1.1
  - Filing and Payment Compliance (F&PC) release 1.1
  - Modernized e-File (MeF) release 3.2

against best practices related to eliciting, documenting, verifying and validating, and managing requirements.

See GAO-06-310

Internal Revenue Service: System Acquisition/Development

For example, to determine how the agency managed its requirements through the life cycle, we reviewed the following documents:

- baseline requirements
- requirements traceability matrices
- changes to requirements
- impact assessments
- root cause analyses of requirements changes

We attempted to

(1) trace requirements through the life cycle (from initial collection to baseline requirements through testing to the final product),

(2) demonstrate forward and backward traceability of requirements,

(3) track changes to requirements through the approval process, and

(4) determine whether the agency had documented the rationale for the change and its impact.

Internal Revenue Service: System Acquisition/Development

Our findings were:

BSM did not have adequate policies and procedures in place to guide its system modernization projects in developing and managing requirements.

As a result, BSM projects did not consistently follow disciplined requirements development and management practices. Weaknesses in eliciting, documenting, verifying and validating, and managing requirements were found.

For example, related to managing requirements:

- All three projects had a change management process that required approvals, impact analysis and root cause analysis. However, cost and schedule impacts resulting from requirements changes were not tracked or updated.

- Requirements documentation for two of the projects did not demonstrate adequate traceability of requirements from business level requirements to system level requirements to test cases.

IT Human Capital

Legislative Requirements

Human capital centers on viewing people as assets whose value to an organization can be enhanced by investing in them. As the value of people increases, so does the capability of the organization—and therefore its value to clients and other stakeholders.

According to the Clinger-Cohen Act of 1996, to maintain and enhance the capabilities of IT staff, an organization should conduct four basic activities:

- **Requirements**—annually assess the knowledge and skills needed to effectively perform its IT operations to support its mission and goals
- **Inventory**—determine the knowledge and skills of current IT staff to identify gaps in needed capabilities
- **Workforce strategies and plans**—develop strategies and implement plans for hiring, training, and professional development to fill gaps
- **Progress evaluation**—evaluate the progress made in improving IT human capital capability, and use the results of these evaluations to continuously improve the organization's human capital strategies

IT Human Capital

Legislative Requirements

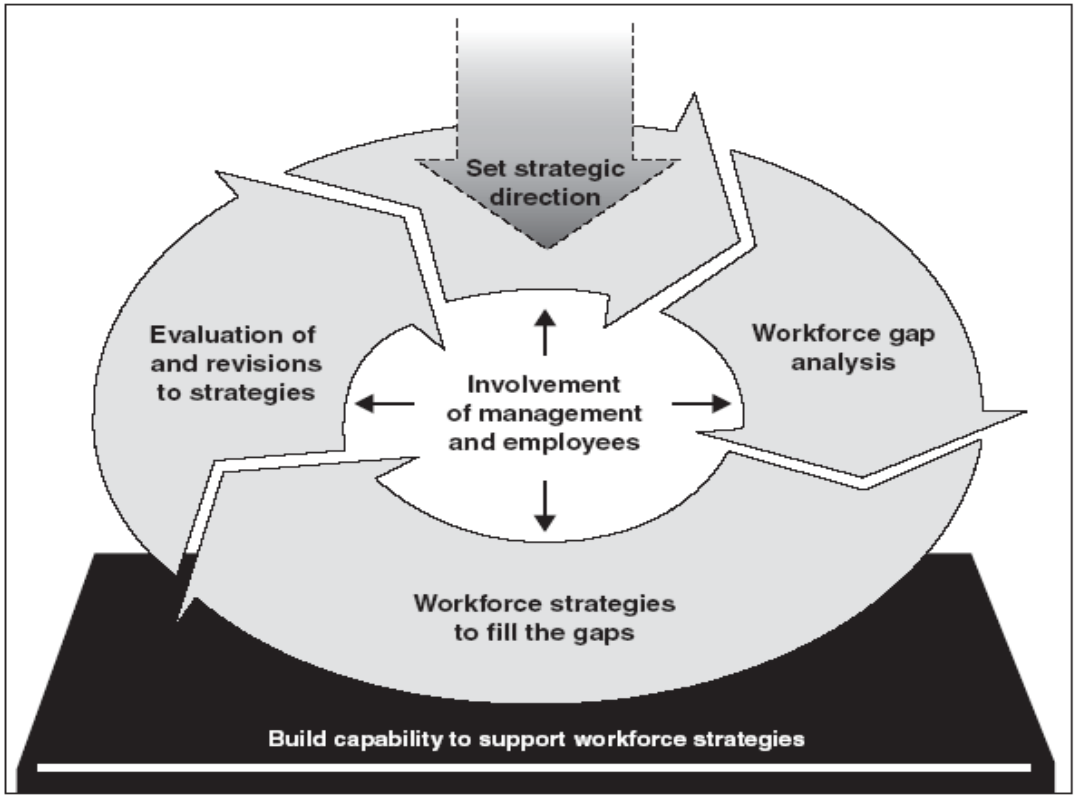
The E-Gov Act of 2002 extends the Clinger-Cohen Act requirements in the area of training. It requires

- Agencies to establish IT training programs that have curricula covering a broad range of IT disciplines; are developed and applied according to rigorous standards; and maximize efficiency through use of a variety of training methods.
- OPM to assess governmentwide IT skills needs and gaps (in practice, agencies may use OPM's survey results also)
- OMB to collect information on the IT workforce from agencies

GAO
Accountability * Integrity * Reliability

Best Practice

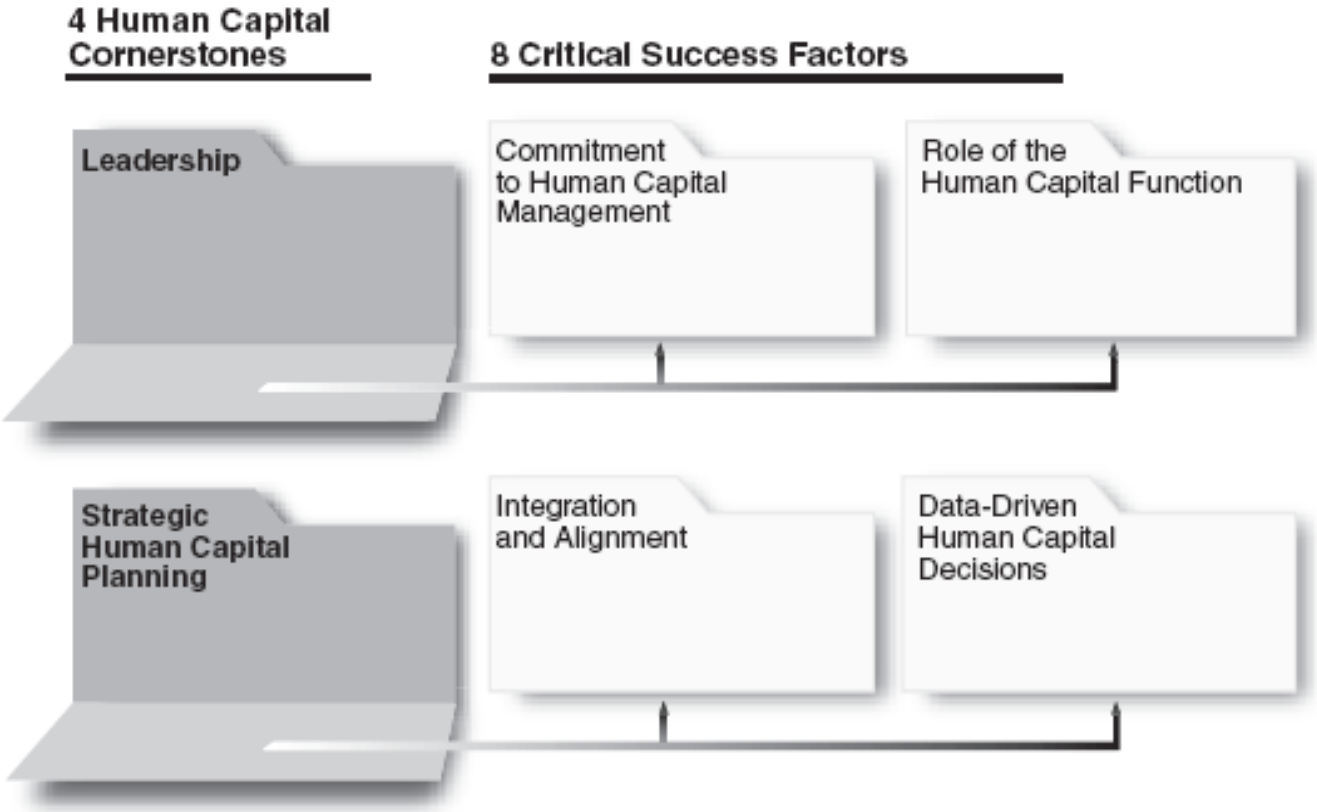
Strategic Workforce Planning Process


Set strategic direction
Workforce gap analysis
Workforce strategies to fill the gaps
Build capability to support workforce strategies
Evaluation of and revisions to strategies
Involvement of management and employees

Source: GAO.

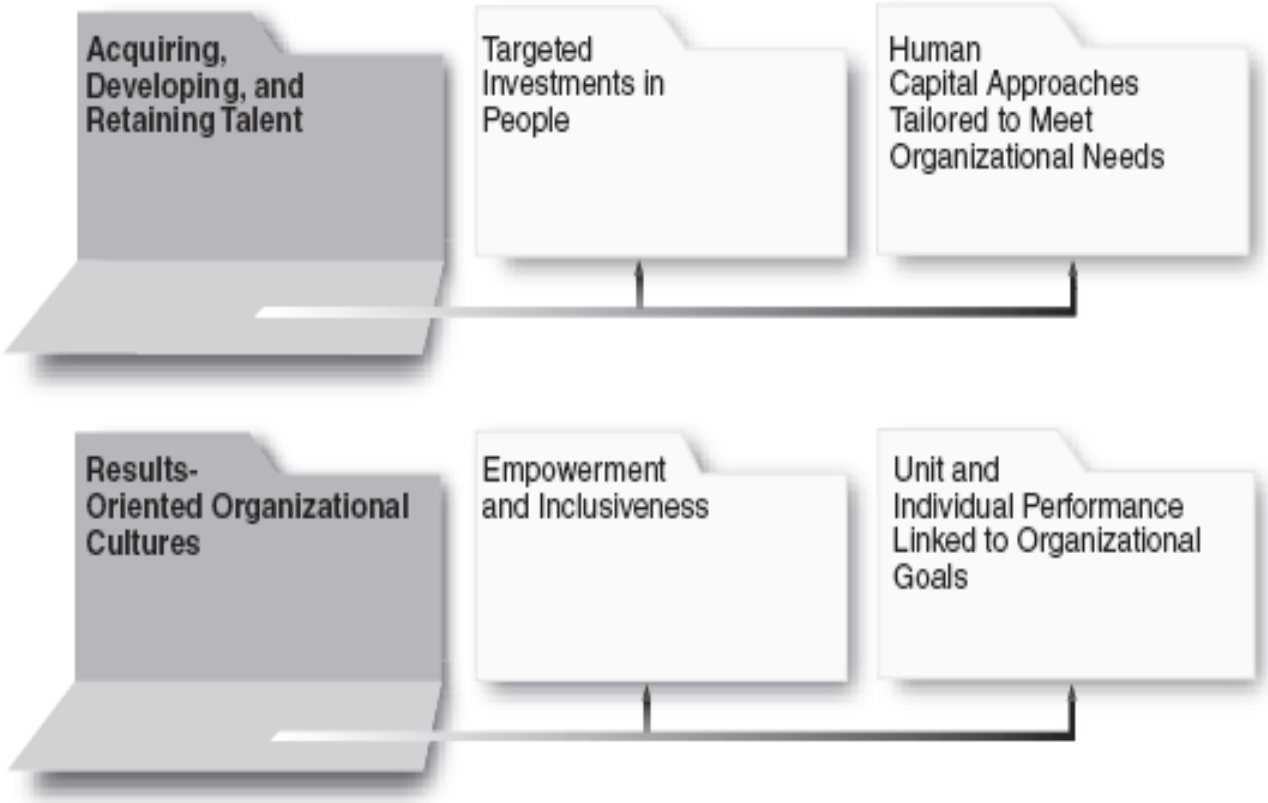
GAO
Accountability * Integrity * Reliability

Critical Success Factors



GAO
Accountability * Integrity * Reliability

Critical Success Factors (cont'd)


Acquiring, Developing, and Retaining Talent
Targeted Investments in People
Human Capital Approaches Tailored to Meet Organizational Needs
Results-Oriented Organizational Cultures
Empowerment and Inclusiveness
Unit and Individual Performance Linked to Organizational Goals

See GAO-02-37SP

U.S. Census Bureau

Human Capital Management

As part of an IT profile of the Census Bureau, we evaluated the adequacy of the Bureau's IT policies, procedures, and practices in key areas including human capital

We compared the bureau's policies and procedures for IT human capital to the Clinger-Cohen Act and to our guide, *Human Capital: A Self-Assessment Checklist for Agency Leaders*. We reviewed IT human capital practices in the areas of skills and knowledge requirements, skills and knowledge inventories, workforce strategies, and progress evaluations.

See GAO-05-661

Human Capital Management

The Census Bureau had implemented steps to manage its IT human capital, such as maintaining an inventory of IT staff skills, but more remained to be done to

- update requirements for IT skills and knowledge and to
- develop and implement strategies for filling any skill gaps.

Until the bureau completes these activities, it is at increased risk that it will not have the skills it needs.

We recommended that the Bureau

- annually assess IT knowledge and skills to determine whether they meet current requirements, and
- use the planned gap analysis to identify workforce strategies to fill skills gaps and then evaluate these strategies to determine their effectiveness in improving human capital management.

Recent Report on IT Human Capital Concerns with FBI's Sentinel Project

In a report on FBI's Sentinel project, a successor to its failed Virtual Case File project, we evaluated whether the FBI is adequately providing for the program's human capital needs. We applied Clinger Cohen Act requirements as embodied in our strategic workforce planning process (see slide 32)

We found the FBI has filled most positions, largely with contractor staff; however the staffing plan addresses only immediate, not strategic needs. It

- Does not inventory skills, forecast future skills needs, or analyze gaps as required by Clinger-Cohen
- Does not have strategies for filling gaps (training, hiring, appropriate reliance on contractors) as required by Clinger-Cohen
- Is not managing human capital as a risk
- Is not derived from fact-based methodology

See GAO-07-19

Training

Leading Practices

In two reports on IT training we studied how training programs mandated by the E-Gov Act were being carried out. In a report on leading practices in the private sector, we identified leading practices in training in five major areas based on our Strategic Workforce Planning Process

- Aligning IT Training with business goals (strategic direction)
- Identifying IT Training Needs (gap analysis)
- Allocating Training Resources
- Design and Delivery (strategies to fill gaps)
- Evaluation

See GAO-03-390, GAO-04-791

Training

Leading Practices (cont'd)

However, in our later, governmentwide study of how well agencies were implementing IT Training programs we found that agencies weren't using most of these practices

- Only 5 of 22 leading practices were widely used
- In two areas—Identifying Needs and Evaluation—agency use of key practices was particularly low
- Funding and finding time for training were the chief obstacles mentioned by agencies

Greater use of leading practices, and strategies to adjust time and funding issues, (such as building training requirements into project and program planning and increasing the use of e-learning and non-classroom delivery methods to reduce cost) would improve federal training management.

Training Leading Practices in the Two Areas Most in Need of Attention

Identify and Assess Training Needs

- Identify and document competencies/skills required for each job description
- Maintain a current inventory of skills
- Address overall career development issues as well as skill-specific training
- Perform a gap analysis to determine where training is needed
- Use self-directed tools, such as IDPs,
- Use a single portal to give staff and managers access to training and career development information

Evaluate Training

- Collect information on how job performance is affected by training
- Validate IT content learning by testing and certification of specific skills
- Assess evaluation results in terms of business impact

Information Security

Information Security

- Goals: Confidentiality, Integrity, Availability

- Increased Risks in Information Systems
  - Dollars passing through automated systems are rising
  - Increased complexity of systems
  - Preponderance of defective software
  - Availability of hacking tools/increased hacking

- What's at stake
  - Disruption of critical operations
  - Loss, misuse or modification of data and/or resources
  - Release of sensitive information
  - Fraud
  - Embarrassment
  - Civil or criminal penalties

Information Security

- GAO's Information Security Audit Methodology is documented in the Federal Information System Controls Audit Manual (FISCAM).

- Methodology for efficiently and effectively evaluating the effectiveness of information security controls
  - Risk-based
  - Organized to facilitate
    - Audit planning
    - Evaluation of findings
    - Audit report drafting
  - Draws on previous IS audit experience
- Currently under revision

FISCAM Chapters 1 and 2

- Chapter 1 – Introduction
  - Nature of IS controls, determining audit procedures, and legislative reforms
- Chapter 2 – Performing the information security audit
  - Planning the IS audit, performing IS audit tests, reporting audit results, and documentation

FISCAM Chapters 3 and 4

- Describe broad control areas
- Identify critical elements of each control area and related control activities
- List common types of control techniques
- List suggested audit procedures

GAO
Accountability * Integrity * Reliability

Example of Control Activities/Techniques and Audit Procedures

Control Activities	Control Techniques	Audit Procedures
SP-3.3 Owners and users are aware of security policies	An ongoing security awareness program has been implemented. It includes first-time training for all new employees, contractors, and users, and periodic refresher training thereafter. Security policies are distributed to all affected personnel, including system/application rules and expected behaviors.	Review documentation supporting or evaluating the awareness program. Observe a security briefing. Interview data owners and system users. Determine what training they have received and if they are aware of their security-related responsibilities. Review memos, electronic mail files, or other policy distribution mechanisms. Review personnel files to test whether security awareness statements are current.

Information Security

GAO
Accountability * Integrity * Reliability

Six general control areas :

- Entity-wide Security Program Planning and Management (SP)
- Access Control (AC)
- Application Software Development and Change Control (CC)
- System Software (SS)
- Segregation of Duties (SD)
- Service Continuity (SC)

Entity-wide Security Program Planning and Management (SP)

- Establish a security management program
- Periodically assess and validate risks
- Document security control policies and procedures
- Ensure owners, administrators, and users are aware of security policies and effectively trained
- Monitor, test, and evaluate the effectiveness of security controls
- Implement remedial actions as needed
- Implement effective incident handling policies
- Ensure that activities performed by external third parties are adequately secure

Access Control (AC)

- Adequately protect information system boundaries
- Implement effective identification and authentication mechanisms
- Implement effective authorization controls
- Encrypt sensitive system resources as appropriate
- Implement an effective audit and monitoring capability
- Establish adequate physical security controls

Application Software Development and Change Control (CC)

- Develop and document CM policies, plans, and procedures
- Maintain current configuration identification information
- Properly authorize, test, approve, and track all configuration changes
- Routinely monitor the configuration
- Update software on a timely basis to protect against known vulnerabilities
- Appropriately document and approve emergency changes to the configuration

System Software (SS)

- Limit access to system software
- Monitor access to and use of system software
- Control changes to system software

Segregation of Duties (SD)

- Segregate incompatible duties and establish related policies
- Establish access controls to enforce segregation of duties
- Control activities through operating procedures, supervision and review

Service Continuity (SC)

- Prioritize among operations and identify supporting resources
- Mitigate potential threats
- Develop and document a comprehensive contingency
- Periodically test plan and adjust as appropriate

Questions & Answers

Presenters

- Randy Hite, Director, Information Technology Architecture and Systems Issues, *hiter@gao.gov*
- Neela Lakhmani, Assistant Director, *lakhmanin@gao.gov*
- Tomas Ramirez, Senior IT Analyst, *ramirezt@gao.gov*
- Tonia Johnson, Assistant Director, *johnsontl@gao.gov*
- Glenn Spiegel, Senior Analyst, *spiegelg@gao.gov*
- Tammi Nguyen, Senior Analyst, nguyentl@gao.gov